数理解析研究所講究録
179巻 1973年 45-61

Automorphism group of a factor automaton

早大 理工　　植村 憲治

Factor Automaton の automorphism group についての研究は Fleck[5], Bayer[6], Paul[7] によって行なわれており，Fleck は strongly connected automaton $A=(S, \Sigma, M)$ について H が G(A) の normal subgroup である時，$G(A)/H$ は $G(A/H)$ の subgroup に isomorphic を示し，Bayer は H が normal でない一般の場合について論じた．又 Paul は S 上の2つの permutation group を定義する事によって $G(A/H)$ と isomorphic な group をみつけている．

Fleck の結果より G/H と isomorphic な subgroup をふくむ任意の group L に対して $G(A)=G$, $G(A/H)\cong L$ となる automaton が存在するか，という問題が生じてくる。

ここではその必要条件を述べる．

次に基本的な事項を列挙する。

$\# S$: set S の cardinality.

$\#A$: automaton $A=(S,\Sigma,M)$ の S の cardinality 即ち $\#S$

S_1+S_2 : $S_1\cup S_2$ の意味だが $S_1\cap S_2=\phi$ が成り立っている.

定義1 automaton A とは $A=(S,\Sigma,M)$ である。S は finite nonempty set of states, Σ は finite nonempty set of symbols, M は $S\times\Sigma\to S$ の mapping である.

Σ^* で Σ の element による finite sequence の全体と empty sequence λ による set を表わす。

M は $S\times\Sigma^*\to S$ の mapping に次の様に拡張される.

$$M(s,\lambda)=s,\quad M(s,x\sigma)=M(M(s,x),\sigma)\quad x\in\Sigma^*,\sigma\in\Sigma$$

定義2 automaton $A=(S,\Sigma,M)$ が strongly connected とは $^\forall s,{}^\forall t\in S$ に対して $^\exists x\in\Sigma^*$ で $t=M(s,x)$ が成り立つ時をいう.

定義3 $A=(S,\Sigma,M)$ を automaton とする。S 上の permutation g が A の automorphism であるとは, $M(s,x)g=M(sg,x)$ for any $s\in S$, $x\in\Sigma$ が成り立つ時をいう。

定義4 set S 上の permutation group G が regular permutation group であるとは, $sg=s$ for some $s\in S$ ならば g は G の identity である permutation をいう.

automaton A の automorphism の全体は permutation の演算に関して S 上の permutation group になっている事が

容易に示され，これを$G(A)$と書き，automaton Aのautomorphism groupと呼ぶ。Aがstrongly connectedの時$G(A)$はS上のregular permutation groupになる事が容易に示される。

<u>定義5</u>　S上のpermutation group Gが与えられて$^\forall s, ^\forall t \in S$に対して$^\exists g \in G$, $s = tg$が成り立つ時Gはtransitiveという。

<u>定義6</u>　$A=(S,\Sigma,M)$をautomatonとする。$G(A)$のsubgroup Hに対してSのpartition $S/H=\{s_1H, s_2H,\cdots, s_mH\}$を考える。この時$S=s_1H+s_2H+\cdots+s_mH$になっている訳である。

$A/H=(S/H,\Sigma,\bar{M})$なるautomatonが次の様に定義される。

$$\bar{M}(s_iH,\sigma)\overset{def}{=}M(s_i,\sigma)H.$$

これは$M(s_i,\sigma)H=M(s_iH,\sigma)$ゆえwell-definedである。

このautomaton A/HをAのHによるfactor automatonと呼ぶ。

$\Sigma^*-\{\lambda\}$上に$x\sim y \Leftrightarrow M(s,x)=M(s,y)$ for any $s\in S$でrelationを定義するとこれはequivalence relationとなりS上のmappingのsemigroupをinduceする。このsemigroupをautomaton Aのcharacteristic semigroupと呼ぶ。

<u>定義7</u> group G と subgroup H が与えられた時，
$N(H)=\{a \mid a^{-1}Ha=H\}$ は G の subgroup となり，H の normalizer と呼ぶ．H は $N(H)$ の normal subgroup になる。特に G を示す必要のある時には $N_G(H)$ と書く．

<u>定義8</u> group G と normal subgroup H が与えられて Γ が G/H に isomorphic な group の時 G は H の Γ による extension という．

<u>定義9</u> group K が H の K/H による extension であって group G をふくむ時，K は H の K/H による G をふくむ extension と呼ぶ。

<u>定理1</u> 任意の group G に対して G 上の permutation group G_R と G_L が存在して，

i) G_R, G_L は G 上 transitive regular,

ii) $g_R h_L = h_L g_R \qquad g_R \in G_R,\ h_L \in G_L$

iii) $G_R \cong G \cong G_L$

iv) G_R の各 element と可換な G 上の permutation の全体は G_L.

v) $G_R \to G_L$ の isomorphism φ が存在して G_R の normal subgroup を H_R とすると $H_L=\varphi(H_R)$ で，G の H_R による partition と H_L による partition は同じものになり，G_R/H_R, G_L/H_L は G/H_R 上の regular permutation group となり, $gh = hg$ $\forall g \in G_R/H_R$, $\forall h \in G_L/H_L$

である。

証明. $g \in G$ に対して G_R, G_L の element g_R, g_L を次の様に定義する。

$$x g_R = xg$$
$$x g_L = g^{-1}x \qquad x \in G.$$

すると g_R, g_L は G 上の permutation となり, G_R, G_L は G 上の permutation group となる.

i) 任意の g, h に対し $g \cdot g^{-1}h = h$ であるから

$g(g^{-1}h)_R = h$ となり G_R は transitive,

$x g_R = x$ for some x の時

$xg = x \quad \therefore g = e \quad \therefore y g_R = y$ for any $y \in G$

となって G_R は regular である.

G_L についても同様である.

ii) $x g_R h_L = xg h_L = h^{-1}xg = h^{-1}x g_R = x h_L g_R$

$\therefore g_R h_L = h_L g_R$

iii) $g \mapsto g_R, g \mapsto g_L$ は $G \to G_R$, $G \to G_L$ の isomorphism を与えている事が容易にわかる。

iv) h が G 上の permutation で G_R の element と可換で,

$eh = g_1$ とする.

$gh = e g_R h = e h g_R = g_1 g$ となり, e を g_1 に

動かしてG_Rと可換なpermutationはただ1つしか存在しない事になり，それはすでにG_Lの中にある。

v) $\varphi: g_R \mapsto g_L$ を考えるとこれはiii)より$G_R \to G_L$のisomorphismであり，Gのnormal subgroup Hに対してH_R, H_Lを考えると

$\varphi(H_R) = H_L$ である.

この時 $xH_R = xH = Hx = xH_L$

よってH_R, H_LによるGのpartitionは同じものになる.

$g_R \in G_R$ は $(xH)g_R = xHg = xgH$ より

G/H_R 上のpermutationを与え，

$xHg_R = xH$ for any $x \Leftrightarrow g_R \in H_R$ より

kernelはH_Rとなる。即ちG_R/H_RはG/H_R上のpermutation group (にisomorphic)となる。

又 $xHg_R = xH$ for some $x \Leftrightarrow g \in H$ となり

$yHg_R = yH$ for any y となって

G_R/H_R はregular permutation groupになる。

G_L/H_L も同様である.

$g_R h_R k_L h'_L = k_L h'_L g_R h_R \qquad g, k \in G, h, h' \in H$

より $g_R H_R k_L H_L = k_L H_L g_R H_R$ となって

G_R/H_R と G_L/H_L は可換である． Q.E.D.

<u>補助定理1</u> S上の regular permutation group G が与えられた時，G の subgroup H に対して $N(H)/H$ は S/H 上の regular permutation group（に isomorphic）になる．

証明 $S/H = \{s_1H, s_2H, \cdots, s_mH\}$ とする．

S/H 上に permutation を次の様に定義する．

$g \in N(H)$ に対して $(s_iH)\cdot g = (s_ig)H$．

$s_igH = s_iHg$ よりこれは well-defined であり，

g がもともと S 上の permutation であったから g は S/H 上の permutation になっている．

次に $s_iHg = s_iH$ for any s_iH ⟺ $s_igH = s_iH$ for any s_iH

⟺ $\exists h_i$, $s_ih_ig = s_i$ ⟺ $h_ig = id$（G が regular より）

⟺ $g \in H$．よって kernel は H となり，$N(H)/H$ は S/H 上の permutation group（に isomorphic）になる。

又 $s_iHg = s_iH$ for some s_iH ⟺ $s_igH = s_iH$

⟺ $g \in H$ ⟺ $s_jHg = s_jH$ for any s_jH となって $N(H)/H$ は regular になる． Q.E.D.

補助定理1より，S上の regular permutation group G と subgroup H が与えられた時．$N(H)/H$ は S/H 上の regular permutation group と isomorphic になるが，

その S/H 上の group は $N(H)/H$ に depend しているので今後は $N(H)/H$ そのものが S/H 上の regular permutation group と考える。

<u>Remark</u> $(s\cdot H)\cdot \underline{N(H)}/H = s\cdot N(H)$ である。(両辺をSの subset とみて。)

<u>定理2 [6]</u> $A=(S,\Sigma,M)$ を strongly connected automaton, H を $G(A)$ の任意の subgroup とする。

i) $N(H)/H$ は $G(A/H)$ の subgroup に isomorphic であり,

ii) 特に $\# G(A) = \# S$ の時 $N(H)/H$ は $G(A/H)$ と isomorphic になる。

証明は [6] を参照。

定理2において H が normal な場合が Fleck [5] の結果である。

group G, $G\neq\{e\}$ と H が与えられた時に $G(A)\cong G$, $G(A/G(A))\cong H$ となる automaton は単につくる事ができる。この拡張として次の問題が起きてくる。

G, H, L が $H\neq\{e\}$ は G の normal subgroup, L は G/H と isomorphic な subgroup を持つように与えられた時, $G(A)\cong G$, $H'\cong H$ として (H' は $G(A)$ の subgroup) $G(A/H')\cong L$ となる automaton A が存在するか。

一般には無理と思われる。次の定理3がその十分条件を与え

る。

<u>定理3</u>　Kを normal subgroup $H \neq \{e\}$ の K/H による Gをふくむ extension とする。この時 automaton Aが存在して $G(A) = G_R$,　$G(A/H_R) = K_R/H_R$ である。

証明　automaton $B = (K, K, M)$ を考える．Kが states の set で又 symbols の set にもなっている。

$M(k_0, k) = k^{-1} k_0$ で定義する。

この時 $K = G + Gk_2 + \cdots + Gk_m$ という states の set の partition が存在する。

Bに symbol を1つふやした automaton A を考える，

$h \in H\ (h \neq e)$ を1つとって

$$M(k, \bar{h}) = k \quad \text{if } k \in G$$
$$= h^{-1} k \quad \text{if } k \notin G.$$

とする．　$h^{-1}G = G$ よりこれはK上の permutation になっている．

$A = (K, K \cup \{\bar{h}\}, M)$ とする．

Bの characteristic semigroup は作り方より K_L であり，よって $G(B) = K_R$ である。

作り方より $G(A)$ は $G(B)$ の subgroup であるから，$e \cdot G(A) = G$（states の subset とみて）をいえば $G(A) = G_R$ になる．

i) $e \cdot g = k' k_i$ とする ($g \in G(A)$, $k_i \neq e$, $k' \in G$)

$k' k_i = e \cdot g = M(e, \tilde{h}) g = M(e \cdot g, \tilde{h}) = M(k' \cdot k_i, \tilde{h})$

$= h^{-1} k' k_i \neq k' k_i$. よって $e \cdot G(A) \subset G$.

ii) $g_R \in G_R$ をとると

$$M(k, \tilde{h}) g_R = k g = M(k g, \tilde{h}) \quad \text{if } k \in G$$
$$= h^{-1} k g = M(k g, \tilde{h}) \quad \text{if } k \notin G$$

より $g_R \in G(A)$ となり $G_R \subset G(A)$ となって

$G = e \cdot G_R \subset e \cdot G(A)$ である.

よって $G(A) = G_R$ である.

次に $A/H_R = (K/H_R, K \cup \{\tilde{h}\}, \bar{M})$,

$B/H_R = (K/H_R, K, \bar{M})$ を考える.

$k' \in K$ に対して

$$\bar{M}(k H_R, k') = M(k, k') H_R$$

$\tilde{h}$ に対して

$$\bar{M}(k H_R, \tilde{h}) = H \quad \text{if } k H_R = H$$
$$= h^{-1} k H_R = h^{-1} k H = h^{-1} H k$$
$$= H k = k H \quad \text{if } k H_R \neq H.$$

よって $\bar{M}(k H_R, \tilde{h}) = k H_R$ となり, $\tilde{h}$ の与える transition は $e \in K$ の与える transition と同じである。B/H_R は A/H_R の symbols から $\tilde{h}$ を除いたもので, transition には何の違いもないから, characteristic semigroup は同じものになり，states の set も同じ事から automorphism group も等しくなって

$G(A/H_R) = G(B/H_R)$.　B は $G(B) = K_R$ より Fleck の結果より $G(B/H_R) = K_R/H_R$.

よって $G(A/H_R) = K_R/H_R$　　　Q.E.D.

定理 4　$A = (S, \Sigma, M)$ を strongly connected automaton とし，$G(A) = G$，H は G の normal subgroup とする．その時 $G(A/G)$ は $N(G/H)/G/H$ と isomorphic な subgroup をもつ．ただし $N(G/H)$ は $G(A/H)$ の中で考える．

証明　$A/G = (S/G, \Sigma, \overline{M})$

$A/H = (S/H, \Sigma, \overline{\overline{M}})$ とする。

$g \in N(G/H)$ として $sG \cdot g \overset{def}{=} (sH)\cdot(G/H)g$ とすると

$(sH)\cdot(G/H)g = (sH)\cdot g(G/H) = s'H\cdot(G/H) = s'G$ ゆえ

これは well-defined.

$\overline{M}(sGg, x) = \overline{M}((sH)(G/H)g, x) = \overline{\overline{M}}((sH)G/H\,g, x)$

$= \overline{\overline{M}}((sH), x)\,G/H\,g = M(s, x)\,H\cdot G/H\,g = M(s, x)\,G\cdot g$

$= \overline{M}(sG, x)\,g$.

又 $sGg = sG$ for any $sG \Leftrightarrow (sH)(G/H)g = (sH)(G/H)$

$\Leftrightarrow g \in G/H$.　よって $N(G/H)/(G/H)$ は $G(A/G)$ の subgroup（に isomorphic）である．

Q.E.D.

<u>定理5</u>　定理3でつくられた automaton A について

$G(A/G_R) \cong N_{K_R/H_R}(G_R/H_R)/G_R/H_R$ である．

証明．$G(A/H_R) = K_R/H_R$ は G_R/H_R をふくむから

$(A/H_R)/G_R/H_R = ((K/H_R)/G_R/H_R, K^{\cup}\{\varepsilon\}, \bar{\bar{M}})$ が定義でき，又 $A/G_R = (K/G_R, K^{\cup}\{\varepsilon\}, \bar{\bar{M}})$ である．

$(A/H_R)/G_R/H_R$ の states も A/G_R の states も K 上の partition を induce するが，Remark より

$(k H_R)\cdot G_R/H_R = k\cdot G_R$ となって両者の partition は同じものになる．

$\bar{\bar{M}}((kH_R)\cdot G_R/H_R; k') = \bar{M}(kH_R, k')G_R/H_R = M(k,k')H_R\cdot G_R/H_R$

$\bar{\bar{M}}(kG_R, k') = M(k,k')G_R$ となって

$(kH_R)\cdot G_R/H_R \mapsto kG_R$ は $(A/H_R)/G_R/H_R \to A/G_R$ の isomorphism を与える．

即ち $G(A/G_R) \cong G(A/H_R/G_R/H_R)$.

$\# G(A/H_R) = \# A/H$ と定理2より

$G(A/H_R/G_R/H_R) = N_{K_R/H_R}(G_R/H_R)/G_R/H_R$.

である。

即ち $G(A/G_R) \cong N_{K_R/H_R}(G_R/H_R)/G_R/H_R$.

Q.E.D.

これは定理3の A が条件を満しつつ，$G(A/G(A))$ が可能なかぎり一番小さい automaton になっている事を意味する。

HがG(A)でnormalの条件をはずすとどうなるかはまだ全然分っていない。

<u>系6</u>　GがΓとHのdirect productである時，Γとisomorphicなsubgroupをもつ任意のgroup Lに対してautomaton Aが存在して　$G(A)=\bar{G}\cong G$, $G(A/\bar{H})\cong L$ である．

$\bar{H}$は$\bar{G}$のsubgroupでHに対応するもの。

証明．定理3のKとしてL×Hをとればよい。

定理3より得られる別の十分条件を示す前に群論の知識が必要である。以下はSchreierの定理と呼ばれるもので，詳しくは群論の本を参照していただきたい。

group GがHのΓによるextensionとする．

$\Gamma\to G/H$のisomorphismを1つ固定して

$\xi\mapsto r_\xi H$　とする　$r_\xi\in G$．

$G=\bigcup_{\xi\in\Gamma} r_\xi H$　である。

$r_\xi H\, r_\eta H=r_{\xi\eta}H$　より

$r_\xi\cdot r_\eta=r_{\xi\eta}\,c_{\xi,\eta}$ 　$c_{\xi,\eta}\in H$　…… (1)

が成り立つ．

次に　$r_\xi^{-1}\,a\,r_\xi=a^\xi$　　$a\in H,\ \xi\in\Gamma$　… (2)

で表わす．　a^ξ はHのautomorphismになっている．

$c_{\xi,\eta}$ $(\xi,\eta\in\Gamma)$ をtransversal $\{r_\xi\}$に関するGのextensionのfactor systemと呼ぶ。

$a \to a^\xi$ の automorphisms は $\{r_\xi\}$ に関する G の automorphism system と呼ばれる。
両者を合わせて $\{c_{\xi,\eta}; a \to a^\xi\}$ は G の transversal $\{r_\xi\}$ に関する parameter system と呼ばれる。
すると G の演算は

$$r_\xi a r_\eta b = r_\xi r_\eta a^\eta b = r_{\xi\eta} c_{\xi,\eta} a^\eta b \quad \cdots\cdots (3)$$
$$(c_{\xi,\eta} a^\eta b \in H)$$

であらわされる.
さらに(1), (2)より $(a^\xi)^\eta = (a^{\xi\eta})^{c_{\xi,\eta}} \quad \cdots (4)$
がいえる. ここに $x^y = y^{-1}xy \quad (x, y \in H)$ とする.
又 associative law より

$$c_{\xi,\eta\zeta}\, c_{\eta,\zeta} = c_{\xi\eta,\zeta}\, c_{\xi,\eta}^{\zeta} \quad (\xi, \eta, \zeta \in \Gamma) \cdots (5)$$

がいえる。
よってすべての parameter system は (4), (5) の関係を満している,
逆に group H と Γ があって
i) Γ の elements の任意の pair (ξ, η) に対して $c_{\xi,\eta}$ で表わされる H の element が1つ存在し
ii) H の automorphism $a \to a^\xi$ が任意の $\xi \in \Gamma$ に定義されて,
それらが (4), (5) の条件を満す時, H の Γ による extension

group がつくられ，G の element を $r_\xi a$ の形であらわして演算は

$r_\xi a r_\eta b = r_{\xi\eta} c_{\xi,\eta} a^\eta b$ となる．

定義10．G が H の Γ による extension で $c_{\xi,\eta} = e$ for any $\xi, \eta \in \Gamma$ が成り立っている時 transversal $\{r_\xi\}$ は G の subgroup R となって $G = RH$，$R \cap H = \{e\}$ である．又逆にこの時 R は transversal となって H の R による extension $c_{\xi,\eta} = e$ であって G と isomorphic な group がつくられる．

$G = RH$　$R \cap H = \{e\}$　H は G の normal subgroup が成り立っている時 G は normal subgroup H と R の semidirect product という．

補助定理2　group G が H の Γ による extension とし，L が normal subgroup M と Γ の semidirect product とする時 H の L による G と isomorphic な group をふくむ extension K が存在する．

証明　$\Gamma \to G/H$ の isomorphism を固定し，その transversal $\{r_\xi\}$ に関する parameter system を

$\{c_{\xi,\eta} ; h \to h^\xi\}$ とする．

$(h^\xi)^\eta = (h^{\xi\eta})^{c_{\xi,\eta}}$，

$c_{\xi,\eta\zeta} c_{\eta,\zeta} = c_{\xi\eta,\zeta} c_{\xi,\eta}^\zeta$ が成り立つ．

又 $(r_\xi h)(r_\eta k) = r_{\xi\eta} c_{\xi,\eta} h^\eta k$ である．

Lのelementはξa $a\in M$の形である.
HのLによるextensionを考えるために
parameter systemを

$$h \to h^{\xi a} \underset{=}{\text{def}} h \to h^{\xi}$$

$$C'_{\xi a, \eta b} \underset{=}{\text{def}} C_{\xi,\eta}$$ とする.

あきらかに $h \to h^{\xi a}$ はHのautomorphismであり,

$C'_{\xi a, \eta b} \in H$である.

これらが(4), (5)を満す事をいってさらにGにisomorphicなsubgroupをふくむ事をいえばよい.

$$(h^{\xi a})^{\eta b} = (h^{\xi})^{\eta} = (h^{\xi\eta})^{C_{\xi,\eta}} = (h^{(\xi a)(\eta b)})^{C'_{\xi a,\eta b}}.$$

$$C'_{\xi a, \eta b \zeta c} C'_{\eta b, \zeta c} = C_{\xi, \eta\zeta} C_{\eta,\zeta} = C_{\xi\eta,\zeta} C_{\xi,\eta}^{\zeta}$$

$$= C'_{(\xi a)(\eta b), \zeta c} C'^{\,\zeta c}_{\xi a, \eta b}$$ である.

よって(4), (5)が満たされた.

次にKのelementは$r_{\xi a} h$とあらわされるから

$G' = \{ r_{\xi e} h,\ \xi \in \Gamma,\ h \in H \}$ とする.

$$(r_{\xi e} h)(r_{\eta e} k) = r_{\xi\eta, e} C'_{\xi e, \eta e} h^{\eta e} k$$

$$= r_{\xi\eta, e} C_{\xi,\eta} h^{\eta} k$$ となり,

$r_{\xi} h \mapsto r_{\xi e} h$ は $G \to G'$ のisomorphismを与える事がわかる。 Q. E. D.

<u>定理7</u> group G と normal subgroup H に対し group L が normal subgroup M と G/H に isomorphic な subgroup の semidirect product になっている時, automaton $A=(S,\Sigma,M)$ が存在して $G(A)=\bar{G}\cong G$, $G(A/\bar{H})\cong L$ である. $\bar{H}$ は $\bar{G}$ の中で H に対応する group である.

証明は補助定理2と定理3よりあきらかである。

文献

1. Weeg,G.P. "The structure of an automaton and its operation-preserving transformation group", J.ACM 9 p345 1962

2. Fleck,A.C. "Isomorphism groups of automata", J.ACM 9 p468 1962

3. Oehmke,R.H. "On the structure of an automaton and its input semigroup", J.ACM,10 p521 1963

4. Barnes,B "Groups of automorphisms and sets of equivalence classes of input for automata", J.ACM,12 p561 1965

5. Fleck,A,C, "On the automorphism group of automata", J.ACM, 12 p566 1965

6. Bayer,R "Automorphism groups and quotients of strongly connected automata and monadic algebras", IEEE Conf. Rec. 1966 7th Ann. Symp. on Switching and Automata Theory 1966

7. Paul,M. "On the automorphism group of a reduced automaton", IEEE Conf. Rec. 1966 7th Ann. Symp. on Switching and Automata Theory 1966

8. Bavel,Z, "Structure and transition preserving functions of finite automata" J.ACM, 15 p135 1968

9. Barnes,B "On the group of automorphisms of strongly connected automata" M.S.T. 4, p289 1970

10. 植村 "Regular permutation group と strongly connected automaton automorphism group について" 数理解析研講究録 123 p68 1971

11. Burnside,W "Theory of groups of finite order" 2nd ed. Dover Publications Inc., New York 1955

12. Kochendörffer,R "Group Theory" McGraw-Hill London 1970